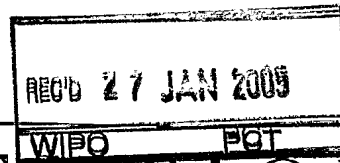




PCT/FR 2004/002872



BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 18 NOV. 2004

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS
CONFORMÉMENT À LA
RÈGLE 17.1.a) OU b)

Martine PLANCHE

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE
26 bis, rue de Saint-Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr





BREVET D'INVENTION

CERTIFICAT D'UTILITE

26bis, rue de Saint-Petersbourg
75800 Paris Cédex 08
Téléphone: 01 53.04.53.04 Télécopie: 01.42.94.86.54

Code de la propriété intellectuelle-livre VI

REQUÊTE EN DÉLIVRANCE

DATE DE REMISE DES PIÈCES: N° D'ENREGISTREMENT NATIONAL: DÉPARTEMENT DE DÉPÔT: DATE DE DÉPÔT:	Philippe KOHN CABINET PHILIPPE KOHN 30, rue Hoche 93500 PANTIN France
Vos références pour ce dossier: B-1302-FR	

1 NATURE DE LA DEMANDE

Demande de brevet

2 TITRE DE L'INVENTION

PROCÉDE DE DETECTION ET DE PREVENTION DES USAGES ILLICITES DE CERTAINS PROTOCOLES DE RESEAUX SANS ALTERATION DE LEURS USAGES LICITES

3 DECLARATION DE PRIORITE OU REQUETE DU BENEFICE DE LA DATE DE DEPOT D'UNE DEMANDE ANTERIEURE FRANCAISE

Pays ou organisation Date N°

4-1 DEMANDEUR

Nom: FRANCE TELECOM
 Rue: 6, place d'Alleray
 Code postal et ville: 75015 PARIS
 Pays: France
 Nationalité: France
 Forme juridique: Société anonyme
 N° SIREN: 380 129 866

5A MANDATAIRE

Nom: KOHN
 Prénom: Philippe
 Qualité: CPI: 92-1131, Pas de pouvoir
 Cabinet ou Société: CABINET PHILIPPE KOHN
 Rue: 30, rue Hoche
 Code postal et ville: 93500 PANTIN
 N° de téléphone: 01 41 71 00 10
 N° de télécopie: 01 41 71 01 17
 Courrier électronique: kohn@compuserve.com

6 DOCUMENTS ET FICHIERS JOINTS

	Fichier électronique	Pages	Détails
Texte du brevet	textebrevet.pdf	23	D 20, R 2, AB 1
Dessins	dessins.pdf	4	page 4, figures 6, Abrégé: page 1, Fig.4
Désignation d'inventeurs			

7 MODE DE PAIEMENT				
Mode de paiement		Prélèvement du compte courant		
Numéro du compte client		2250		
8 RAPPORT DE RECHERCHE				
Etablissement immédiat				
9 REDEVANCES JOINTES		Devise	Taux	Quantité
062 Dépôt		EURO	0.00	1.00
063 Rapport de recherche (R.R.)		EURO	320.00	1.00
Total à acquitter		EURO		320.00

La loi n°78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

Signé par

Signataire: FR, Cabinet Philippe Kohn, P. Kohn

Emetteur du certificat: DE, D-Trust GmbH, D-Trust for EPO 2.0

Fonction

Mandataire agréé (Mandataire 1)



BREVET D'INVENTION CERTIFICAT D'UTILITÉ

Réception électronique d'une soumission

Il est certifié par la présente qu'une demande de brevet (ou de certificat d'utilité) a été reçue par le biais du dépôt électronique sécurisé de l'INPI. Après réception, un numéro d'enregistrement et une date de réception ont été attribués automatiquement.

Demande de brevet : X

Demande de CU :

DATE DE RECEPTION	28 novembre 2003	
TYPE DE DEPOT	INPI (PARIS) - Dépôt électronique	Dépôt en ligne: X
N° D'ENREGISTREMENT NATIONAL ATTRIBUE PAR L'INPI	0350929	Dépôt sur support CD:
Vos références pour ce dossier	B-1302-FR	

DEMANDEUR

Nom ou dénomination sociale	FRANCE TELECOM
Nombre de demandeur(s)	1
Pays	FR

TITRE DE L'INVENTION

PROCEDE DE DETECTION ET DE PREVENTION DES USAGES ILLICITES DE CERTAINS PROTOCOLES DE RESEAUX SANS ALTERATION DE LEURS USAGES LICITES

DOCUMENTS ENVOYES

package-data.xml	Requetefr.PDF	fee-sheet.xml
Design.PDF	ValidLog.PDF	textebrevet.pdf
FR-office-specific-info.xml	application-body.xml	request.xml
dessins.pdf	indication-bio-deposit.xml	

EFFECTUE PAR

Effectué par:	P. Kohn
Date et heure de réception électronique:	28 novembre 2003 11:52:11
Empreinte officielle du dépôt	21:C0:5F:3B:50:CE:7F:AF:D3:84:20:A7:C0:4A:8D:A6:E4:69:BA:DD

/ INPI PARIS, Section Dépôt /

SIEGE SOCIAL
INSTITUT 26 bis, rue de Saint Petersbourg
NATIONAL DE 75800 PARIS cedex 08
LA PROPRIETE Téléphone : 01 53 04 53 04
INDUSTRIELLE Télécopie : 01 42 93 59 30

**"Procédé de détection et de prévention des usages illicites de
certains protocoles de réseaux sans altération de leurs
usages licites"**

La présente invention concerne un procédé de détection et
5 de prévention des usages illicites de certains protocoles de
réseaux sans altération de leurs usages licites.

Elle trouve application notamment dans la sécurité des
réseaux IP. Elle apporte une parade efficace à différents types
d'attaques qui se caractérisent par une élévation soudaine du
10 débit du protocole corrompu, attaques par déni de service et
canaux cachés notamment. Elle trouve un usage particulièrement
efficace sur les réseaux publics sans fil en accès payant (hot
spot).

L'invention présente notamment deux aspects. Le débit des
15 protocoles concernés est un critère de détection et un moyen
d'éradication de l'attaque. Dans ce second aspect, l'invention se
base sur l'utilisation d'une fonction de retardement qui fait que
tout paquet reçu par le système est réémis avec un retard. Celui-
ci est négligeable quand il n'y a pas d'attaque et devient
20 important quand une attaque est détectée, au point de rendre le
réseau inutilisable à l'attaquant.

Le procédé de l'invention est indépendant de la technique
sur laquelle le réseau IP est bâti : Ethernet, IEEE 802. 11, GPRS,
etc.

25 Le procédé de l'invention apporte, entre autres, une
solution efficace aux fraudes connues sous le nom de *firewall
piercing* (ou canaux cachés).

Ces techniques de fraudes permettent de faire passer au
travers d'un équipement de filtrage des flux d'information
30 normalement interdits en les encapsulant dans des flux autorisés.
L'invention permet de résoudre ce problème dans les cas difficiles
qui jusqu'alors étaient sans solution.

Le procédé de l'invention présente l'avantage d'empêcher la fraude sans avoir d'influence négative notable sur les usages licites du réseau.

De façon plus générale, toute attaque ou fraude reposant
5 sur un échange inhabituel de données avec l'extérieur d'un réseau local est facilement traitable par la présente invention, pourvu qu'elle provoque une hausse significative du débit normalement consommé par le protocole corrompu.

Ainsi certaines attaques par dénis de services (attaques
10 consistant à rendre un service inutilisable aux autres utilisateurs par pure intention de nuire) peuvent aussi être traitées. Ceci s'applique particulièrement bien aux réseaux, dénommés réseaux "hot spot", le hot spot étant une zone de couverture radiofréquence sur laquelle un terminal convenablement équipé
15 peut se connecter et obtenir un accès au réseau Internet, moyennant le règlement d'une somme payée d'avance ou prélevée sur la facture d'abonnement à un fournisseur d'accès à un réseau de communication comme le réseau GSM du client. Ceci est le cas si le hot spot est interconnecté à un opérateur de
20 réseau mobile pour utiliser l'authentification GSM.

Dans ce dernier cas, une autre attaque possible depuis le hot spot sur la machine qui gère l'authentification des utilisateurs est critique, car c'est précisément le serveur d'authentification du réseau GSM. Les opérateurs de réseaux mobiles redoutent une
25 telle attaque par déni de service, car elle mettrait en péril le fonctionnement du serveur d'authentification du réseau GSM et par effet de bord le réseau GSM lui même.

La présente invention permet de détecter automatiquement un nombre anormalement élevé de requêtes et de les limiter.

30 Des techniques de « firewall piercing » pour transporter des protocoles interdits existent aussi et sont souvent utilisées sur les réseaux d'entreprises. L'invention s'applique préférentiellement aux protocoles de "signalisation" comme DNS, ICMP ou EAP (qui lui transporte une méthode d'authentification),

c'est-à-dire des protocoles qui ne servent qu'à faire fonctionner les autres protocoles de l'Internet, mais ne transportent directement de données utiles appartenant aux utilisateurs. Or ces protocoles de « signalisation » sont très différents des
5 protocoles de transport de données en ce qu'ils fonctionnent à des débits normalement faibles et connus. Si ces protocoles de signalisation venaient à être utilisés lors d'une attaque en tant que protocoles de transport, ceci devrait aboutir à un nombre anormalement élevé de requêtes et de réponses.

10 Mais on remarque que l'invention s'applique aussi à des protocoles de transport. Elle s'applique notamment à la protection de protocoles de transport à bas débit, totalement ou partiellement.

Particulièrement, l'invention permet de traiter les
15 protocoles comme DNS (protocole dit de signalisation). En effet, sur un hot spot public par exemple, il est fréquent que, par défaut, tous les flux soient interdits sauf les protocoles de signalisation, indispensables au démarrage des connexions des utilisateurs (transport des données d'authentification, collecte d'information
20 sur la configuration du réseau, résolution de noms). Ainsi un fraudeur qui voudrait utiliser le hot spot sans payer n'aurait que les protocoles de signalisation pour construire un canal caché. A l'inverse, les protocoles "utiles" comme http ou telnet étant interdits par un firewall tant que l'utilisateur n'est pas autorisé à
25 se connecter, ils ne peuvent pas être utilisés en canal caché pour frauder.

Il existe aussi un autre aspect selon lequel l'invention traite les protocoles comme les protocoles "http" ou « ftp ». En effet, dans son usage courant, le protocole "http" est un protocole
30 qui présente un débit fortement asymétrique : un débit faible du terminal vers le serveur qui correspond à des requêtes et un débit élevé dans l'autre sens qui correspond aux pages html servies en réponse. Si une fraude par canal caché sur http venait à rompre cette caractéristique du débit d'une connexion http, c'est-à-dire si

le débit montant devenait soudainement anormalement élevé alors l'invention serait en mesure de bloquer ce trafic.

Pour atteindre ces objets, la présente invention concerne un procédé de protection de protocoles de réseaux sans altération
5 de leurs usages licites qui consiste, pour un flux de paquets de données d'entrée, à appliquer une fonction de retardement pour chaque paquet, insuffisant pour gêner un usage licite, mais suffisant pour gêner un usage illicite.

Particulièrement, dans un protocole de signalisation,
10 l'invention appliquera une fonction de retardement croissante avec le débit du flux surveillé, de sorte que si l'usage illicite du protocole à titre de transport de données privées vient à dépasser un débit standard, le retard croit indéfiniment ce qui coupe pratiquement le canal en usage illicite sans gêner les autres flux.

15 D'autres caractéristiques et avantages de la présente invention seront mieux compris de la description et des dessins annexés parmi lesquels :

- la figure 1 représente une séquence selon un protocole à protéger ;
- 20 - la figure 2 représente un graphe temporel des débits sur des flux surveillés selon un autre protocole à protéger en cas d'attaque non bloquée et en cas d'attaque bloquée par le procédé de l'invention ;
- la figure 3 est un schéma bloc d'un équipement de
25 traitement de flux à surveiller dans le procédé de l'invention ;
- la figure 4 est un organigramme d'un mode particulier de réalisation du procédé de l'invention ;
- la figure 5 est un schéma expliquant les divers scénarios dans un premier exemple d'application de l'invention ;
- 30 - la figure 6 est un graphe temporelle expliquant un scénario dans un second exemple d'application de l'invention.

On va maintenant décrire deux techniques d'attaques utilisées. La première technique d'attaque est utilisable sur les réseaux de type IP. De tels réseaux, peuvent être des réseaux

d'entreprises, l'Internet ou des "hot spots". La deuxième technique d'attaque, par contre, est spécifique aux réseaux "hot spots", et vise particulièrement le serveur d'authentification GSM interconnecté à un réseau « hot spot ».

5 Généralement, les terminaux connectés à un réseau IP exploité par une entreprise, par un opérateur de télécommunication ou par un fournisseur d'accès à Internet, ne sont pas libres de faire n'importe quel type de connexions. Il existe trois grandes raisons à cela.

10 Une première raison est que le réseau est un réseau de production et on ne souhaite pas que les utilisateurs en fassent un usage détourné à des fins de divertissement, d'enrichissement personnel ou de nuisance à autrui.

15 Une seconde raison est que le réseau est d'usage payant et il convient de n'autoriser que les flux pour lesquels l'utilisateur a réglé un droit.

20 Une troisième raison est qu'autoriser plus de connexions que ce qui est nécessaire pour le bon fonctionnement de l'organisation propriétaire du réseau ne peut être qu'une occasion d'un usage illicite.

25 Une opération de filtrage des flux entrant et sortant du réseau est généralement réutilisée sur des équipements à la frontière du réseau tels que des routeurs filtrants ou des pare-feux (dans la suite, ce genre d'équipement est désigné collectivement sous l'appellation "pare-feux" ou "firewalls"). De plus, pour le bon fonctionnement des protocoles autorisés, ces équipements doivent laisser passer sans restriction d'autres protocoles indispensables tels que le protocole ICMP (RFC 792) ou le protocole DNS (RFC 1034)

30 Or, il existe des outils logiciels qui permettent d'utiliser les protocoles autorisés par les pare-feux pour faire passer des protocoles interdits. Ces techniques sont connues sous le nom de "canaux cachés" ou "firewall piercing" et sont toutes construites sur le même schéma, qui sera décrit à l'aide de la figure 5 qui

présente ce type d'attaque dans le cas où le protocole DNS est utilisé pour transporter des données au travers du firewall :

a) Le pirate laisse un serveur en libre accès quelque part sur Internet, à l'extérieur du réseau sur lequel son terminal est
5 connecté. Ce serveur a deux fonctions:

i. Encapsuler/décapsuler les paquets en provenance de la machine du pirate

ii. Retransmettre le paquet extrait vers son destinataire final et recevoir les paquets de ce même destinataire pour les
10 renvoyer vers le pirate (fonction de relais).

b) Le terminal du pirate copie le paquet de données d'un protocole interdit dans une zone libre d'un paquet d'un protocole autorisé et l'envoie à son serveur qui le traite.

De cette manière, le pirate parvient à faire sortir et entrer
15 du trafic normalement interdit en l'encapsulant dans un paquet d'un protocole autorisé. Cette fraude est redoutable pour deux raisons:

- pratiquement tous les protocoles permettent l'encapsulation,
- 20 - les pare-feux doivent nécessairement laisser passer certains protocoles comme DNS et ICMP qui sont connus pour avoir cette capacité d'encapsulation. Un blocage pur et simple de ces protocoles rendrait d'une part ce réseau non conforme aux recommandations de bon fonctionnement et d'interopérabilités,
25 mais empêcherait un fonctionnement normal pour les utilisateurs légitimes.

Les réseaux de type hot spot qui utilisent la méthode d'authentification par carte SIM reposent sur un protocole de communication appelé "EAP-SIM" qui est défini dans les normes
30 publiées. Ce protocole permet de réaliser une authentification GSM entre un client d'un service hot spot, et un opérateur de téléphonie mobile GSM. L'authentification GSM nécessite quelques ressources (charge système). Un grand nombre de demandes d'authentification peut entraîner une perte de qualité

de service, à la fois pour les clients des services GSM classiques, et pour les clients des services sur les réseaux Wi-Fi.

A la figure 1, on a représenté un schéma d'authentification par la méthode EAP-SIM. Un requérant 1 sur le réseau de communications envoie une requête d'authentification 2 selon un protocole 802.11 vers une ressource d'authentification 3.

La ressource d'authentification exécute une opération d'authentification et produit une réponse d'authentification 4 selon un protocole AAA vers un serveur d'authentification 5. Le serveur d'authentification 5 produit en réponse un message d'authentification 6 qui est transmis selon le protocole SS7 vers un centre d'authentification 7.

En appliquant le schéma EAP-SIM en cas d'une attaque, le mode opératoire est le suivant :

L'attaquant signale au point d'accès qu'il est prêt à s'authentifier (EAPOL_Start);

Le point d'accès demande alors à l'attaquant de lui donner son identité (EAP-Request/Identity);

L'attaquant répond donc avec une identité (Network Access Identifier (REC 2486) ou NAI contenue dans EAP-Response/Identity;

Le point d'accès relaie la réponse de l'attaquant vers le Proxy-RADIUS;

Le proxy-RADIUS analyse le contenu de l'identité NAI et relaie la réponse vers le serveur RADIUS de l'opérateur grâce au contenu du NAI (après le symbole @) ;

Le serveur RADIUS de l'opérateur analyse la requête contenant l'identité NAI (en particulier le code IMSI) ;

Le serveur RADIUS de l'opérateur demande alors à l'attaquant de s'authentifier avec l'authentification GSM (EAP-Request/SIM/Start) via le proxy-RADIUS de l'hot spot visité;

L'attaquant répond donc avec un EAP-Response/SIM/Start (Nonce);

Le proxy-RADIUS relaie alors cette réponse vers le serveur RADIUS de l'opérateur;

Le serveur RADIUS de l'opérateur interroge alors la base d'authentification GSM pour récupérer n triplets GSM (n=2
5 ou 3).

C'est la dernière phase qui est coûteuse ; car elle permet à l'attaquant de faire calculer n triplets GSM.

L'attaque consiste donc à rejouer au maximum le mode opératoire précédent en envoyant un type de paquet initiant la
10 phase d'authentification (paquets EAPOL_Start). Il est alors possible de réaliser une attaque par déni de service par saturation de ressources au niveau du centre d'authentification 7, ce qui met en péril à la fois le réseau hot spot, mais surtout le réseau GSM.

15 Pour remédier aux problèmes liés aux attaques de protocoles de communication, l'état de la technique fournit trois moyens qui sont

- les pare-feux dits "firewalls" ;
- les systèmes de contrôle de débit ; et
- 20 - les systèmes de détection et de prévention des intrusions.

Les firewalls sont les systèmes habituellement utilisés pour contrôler les flux sur un réseau. Ils sont généralement placés en coupure entre deux sous-réseaux et analysent les paquets qui les
25 traversent. Ils sont capables de faire un filtrage à différents niveaux :

- IP/ICMP : le le systèmes analyse le contenu des champs des entêtes (adresse IP sources/destination, type et code ICMP) ;
- IP/TCP UDP: le système analyse le contenu des champs
30 des entêtes (adresse IP sources/destination, port TCP UDP)
- Session : le système fait une analyse complète d'une initialisation de session pour l'établissement d'une communication sur un protocole particulier et ainsi s'assure que les paquets entrants correspondent effectivement a des paquets sortants.

- contenu des données échangées dans les protocoles applicatifs et ainsi interdire certains contenus (ex: URL de sites pornographiques).

Les firewalls ne sont néanmoins pas capables de bloquer
5 les flux issus d'attaques par canaux cachés car ils agissent par filtrage "tout ou rien" si le flux est déclaré valide. Dans ce cas, il passe intégralement ou si le flux est déclaré invalide, aucun paquet ne passe. Or les attaques par canaux cachés sont plus subtiles puisqu'elles utilisent des flux autorisés (voire
10 indispensables comme le DNS). Par conséquent, le seul élément qui permette d'identifier une telle attaque est le débit anormalement élevé auquel fonctionnent ces protocoles licites quand ils sont utilisés pour une attaque par canaux cachés. Aucun firewall ne permet ce genre de critère de filtrage.

15 Par ailleurs, le procédé de l'invention offre un filtrage "auto-adaptatif" du trafic suspect qui permet:

- de bloquer rapidement les flux suspects;
- de relâcher automatiquement le blocage une fois que la situation est revenue à la normale;
- 20 - d'offrir à chaque type d'attaque une réponse adaptée en termes de rapidité de blocage, de limite de débit, de rapidité de relâchement du blocage ainsi qu'il sera décrit plus loin pour la fonction $f()$,

- d'éviter de totalement bloquer un flux légitime, et pourtant
25 trop abondant, en ne faisant qu'un ralentissement du ainsi qu'il sera décrit plus loin sur le mode de fonctionnement "sub-normal"

Le trafic continue donc à passer, même si le service est légèrement dégradé. Un firewall classique le bloquerait complètement.

30 Les systèmes de contrôle de débit permettent d'attribuer une partie de la bande passante totale disponible à un type de flux, notamment pour éviter des situations de congestion. Ils font partie des systèmes de gestion de la qualité de service. Dans une certaine mesure, ces systèmes permettent d'éviter l'utilisation

frauduleuse de la bande passante sur les réseaux. Par exemple, ils permettent de limiter le débit total des requêtes DNS et réduisent ainsi la portée de l'attaque par canaux cachés sur DNS. Un logiciel comme le logiciel open source ipfilter, grâce à son
5 module "limit", offre de telles fonctionnalités de limitation de débit.

Toutefois, cela ne réduit pas complètement au silence un attaquant puisqu'il pourra toujours émettre des données au maximum du débit autorisé par le système.

10 La figure 2 montre la réponse en termes de débit à une attaque par canaux cachés sur DNS.

A la figure 2, on a représenté sur un même graphique temporel :

- le débit 12 caractéristique d'un protocole protégé par le
15 procédé de l'invention quand une attaque survient ;

- le débit 8 caractéristique d'un protocole protégé par un système de contrôle de débit lors de la même attaque ;

- le débit 9 caractéristique d'un protocole sans aucune protection lors d'une même attaque que celle prévue pour les
20 débits 8 et 12.

Lors d'une attaque, le débit augmente relativement rapidement selon une pente 10, puis le trafic reste sensiblement constant avec des oscillations aléatoires autour d'une valeur de débit de régime établi.

25 En appliquant un contrôle de débit un système de contrôle de débit de l'état de la technique, le débit de l'attaquant monte plus lentement que dans le cas précédent puis reste constant, bloqué à une valeur de seuil qui correspond au moins au débit 8 d'un protocole de signalisation le plus exigeant en débit.

30 En appliquant le procédé de l'invention, le débit de l'attaquant passe par un maximum 13 puis décroît jusqu'à s'annuler plus ou moins rapidement ainsi qu'on le décrira plus loin.

On voit bien sur la figure 2 que le système de contrôle de débit ne peut pas faire mieux que limiter la bande passante disponible à l'attaque. En revanche, le procédé de l'invention permet de faire tendre le débit vers zéro avec une vitesse de convergence paramétrable. De ce point de vue, l'invention est
5 bien plus efficace que les systèmes de contrôle de flux pour prévenir les attaques par canaux cachés.

Les systèmes de détection d'intrusions (IDS) fonctionnent par analyse des flux circulant sur les artères au moyen d'une
10 sonde. Celle-ci remonte les données collectées à un système "intelligent" qui les interprète et envoie éventuellement une alarme si quelque chose de suspect se produit. Ces systèmes peuvent aussi éventuellement ordonner à un firewall de couper le trafic.

15 On parle alors de systèmes IDS actifs. Une autre évolution de ces systèmes est connue sous le nom de « système de prévention » des intrusions « IPS ».

Dans ce cas, le système IDS est directement couplé avec un firewall, le flux analysé traversant cet équipement. Cela offre
20 alors des possibilités de coupure du trafic semblable aux systèmes IDS actif, mais plus performantes en temps de réaction. Les principes de détection restent les mêmes, les données pertinentes sur lesquelles l'analyse se base sont généralement des séquences d'envoi de messages connus (appelés les
25 signatures des attaques).

Les systèmes IDS sont connus pour présenter de lourds inconvénients:

- ils sont très chers à cause de la technologie de la sonde qui doit être capable d'analyser de grande quantité de trafic;
- 30 - ils ne sont pas très fiables car, comme tout système de reconnaissance automatique ils émettent des alarmes injustifiées (false positive) et réciproquement laissent passer des attaques (false negative);
- ils ne cherchent à détecter que les attaques connues.

La réponse qu'ils fournissent à une attaque n'est pas satisfaisante. Dans le cas d'un système IDS, une alarme est envoyée à un opérateur humain qui doit réagir en conséquence. La présence permanente d'un opérateur est d'ailleurs impensable
 5 sur un petit réseau. Dans le cas des systèmes IPS, la réponse n'est pas meilleure que celle d'un firewall et on se reportera ci-dessus pour l'analyse.

Le procédé de l'invention peut être implémenté soit dans un équipement spécifique, soit comme une fonction
 10 supplémentaire dans un équipement de traitement de flux déjà présent - comme par exemple un routeur, un pare-feu ou un serveur DNS. Dans tous les cas, il est indispensable que la totalité du trafic à contrôler passe par cet équipement. Un tel équipement de traitement de flux représenté schématiquement à
 15 la figure 3 comporte une interface d'entrée 15 et une interface de sortie 17 et que le trafic arrivant sur l'interface d'entrée est réémis sur l'interface de sortie selon une logique définie par le procédé de l'invention.

Elle repose sur le principe suivant qui est exécuté sur un
 20 processeur 16 de l'équipement de traitement de flux, le flux Fie est réémis sur l'interface de sortie comme flux Fjs avec un délai plus ou moins long, ni trop pour ne pas être perceptible des utilisateurs "honnêtes", ni trop peu pour ne pas permettre à un utilisateur malhonnête de faire circuler des données non
 25 autorisées.

D'un point de vue physique, les deux interfaces peuvent être réalisées sur la même carte réseau.

La distinction entre entrée et sortie est valable pour le trafic allant dans un sens. Si l'invention traite également le trafic
 30 dans l'autre sens, les rôles des interfaces sont intervertis.

Dans le procédé de l'invention, on exécute d'abord la désignation des classes de flux à surveiller.

La désignation des classes flux à surveiller peut se baser sur la valeur de certains champs du paquet IP tel que cela ce

pratique pour la configuration des passerelles IPsec (RFC 2401) ou des firewalls.

Par exemple, on peut retenir une désignation des classes de *flux* par une combinaison des valeurs suivantes: une adresse
5 ou une plage d'adresses IP source, une adresse ou une plage d'adresses IP destination, un protocole de niveau supérieur (UDP, TCP, ICMP...), un numéro de port, une valeur d'un champ dans la partie protocole de niveau supérieur.

De manière générale, tout champ protocolaire lisible et
10 interprétable par l'équipement peut être retenu comme critère de sélection, quelque soit son niveau dans la pile des protocoles.

De manière spécifique, dans le cas où l'invention ne fonctionne que comme un ajout à un service particulier, l'implantation d'un système de désignation de classe de flux
15 complet n'est pas forcément nécessaire. Par exemple si le procédé de l'invention est ajouté à un serveur de résolution de noms DNS dans le but d'empêcher les canaux cachés sur le protocole DNS, alors seule la classe de flux DNS est surveillée, ainsi qu'il sera décrit plus loin. Par conséquent il n'est pas utile
20 de laisser la possibilité de désigner d'autres classes de flux.

Dans un mode de réalisation de l'invention, on exécute un armement du mécanisme de bridage des flux à surveiller.

Quand on détecte, sur l'interface d'entrée 15 de l'équipement de traitement des flux, un flux F_{1e} issu d'une machine particulière et appartenant à une classe de flux à surveiller, on
25 crée dynamiquement un compteur associé à ce flux. Pour le flux indexé N , on note CPT_N le compteur associé.

Dans un mode de réalisation de l'invention, le processeur
16 de traitement des flux met en œuvre un mécanisme de bridage
30 des flux non autorisés.

Chaque fois qu'un paquet de données arrive sur l'interface d'entrée 15, lors d'une étape 21 :

Lors d'une étape 22, on exécute un test de mise sous surveillance, s'il n'appartient pas à un flux sous surveillance,

alors il est réémis immédiatement sur l'interface de sortie 17 lors d'une étape 23.

Lors d'un test 24, on vérifie si le paquet arrivé appartient à un flux sous surveillance.

5 S'il appartient à un flux sous surveillance c'est-à-dire si un compteur CPT_N lui est déjà associé, alors, lors d'une étape 25, le compteur CPT_N est incrémenté d'un pas comme l'unité de 1 et le paquet est réémis sur l'interface de sortie 17 lors d'une étape 23, qui dépend d'une fonction $f()$ prédéterminée dépendant de la
10 valeur en cours du compteur CPT_N après un délai $D_N = f(CPT_N)$.

La fonction $f()$ est appelée fonction de retardement.

Dans un mode de réalisation, à chaque paquet réémis sur l'interface de sortie 17, le compteur CPT_N est décrémenté de un pas, comme l'unité 1, lors d'une étape 26.

15 Dans un mode de réalisation, le procédé de l'invention comporte ensuite un mécanisme de relâchement de la surveillance d'un flux.

Une fois que le compteur CPT_N atteint une valeur suffisamment basse, cela signifie qu'il n'y a plus de tentative
20 d'émission de trafic illicite. Le compteur CPT_N peut alors être supprimé et trafic n'est plus sous surveillance. Cette propriété n'est toutefois pas indispensable, le trafic peut rester sous surveillance indéfiniment.

Si à l'issue du test 24, le paquet n'a pas été identifié
25 comme appartenant à une classe de flux sous surveillance, on attribue à son flux un nouveau compteur CPT_N et on exécute l'étape 25.

La fonction de retardement f n'est pas nécessairement unique pour toutes les classes de flux. Ainsi on pourra retarder un
30 flux DNS avec une fonction f_1 et un flux ICMP avec une fonction f_2 .

La fonction de retardement f doit être au minimum croissante de façon à ce que plus l'attaquant envoie de trafic, plus son trafic est retardé.

Une fonction de retardement f à dérivée seconde positive bloquera très vite le flux de l'attaquant. Par exemple $f(CPT_N) = \exp(\alpha * CPT_N + \beta)$ avec $\alpha \geq 0$.

Dans le cas d'une tentative de saturation de l'équipement
5 de contrôle, un compteur $CPTMAX_N$ peut aussi être utilisé, si le nombre de paquets en attente d'émission dépasse la valeur $CPTMAX_N$ paramétrée par l'administrateur, alors les paquets en attente sont détruits selon un algorithme à choisir. Cette fonctionnalité a pour but d'éviter une saturation des ressources de
10 l'invention.

On présente ici un mode de réalisation du procédé de l'invention implémenté dans un serveur DNS local au réseau à protéger.

On va maintenant décrire l'attaque se développant sans
15 l'intervention du procédé de l'invention.

Un réseau local 30 avec contrôle des flux est souvent construit selon un plan présenté sur le schéma de la figure 5. Le réseau local contient des terminaux, dont un exemplaire est représenté en 34, un serveur DNS, nommé DNS local 31 et un
20 routeur/firewall 32 qui assure l'interconnexion du réseau local 30 avec un autre réseau 33 comme le réseau Internet.

Le routeur/firewall 32 est configuré pour interdire certains flux, par exemple des flux « ftp ». Pour contourner l'interdiction 36, le terminal 34 va encapsuler les paquets « ip » qui
25 transportent le flux « ftp » dans des paquets DNS sur des chemins de flux DNS 37, par exemple, en codant de l'information dans des champs spécifiques du paquet. Il s'assure aussi que la requête DNS ne pourra être traitée que par le serveur DNS pirate 38 sous le contrôle du pirate à l'extérieur du réseau local, en
30 choisissant judicieusement les noms de domaines de la requête. La machine DNS pirate 38 pourra alors transférer les paquets vers le serveur « ftp » 39 demandé par le terminal. Le trafic dans l'autre sens prend exactement le chemin inverse.

En implémentant l'invention sur le serveur DNS local, les attaques par canaux cachés sur DNS seront complètement bloquées.

1) Dans ce cas précis décrit à la figure 5, il n'y pas besoin
5 d'implémenter une gestion des classes de flux et des flux sous surveillance. En effet, seuls les flux DNS passent par cette machine.

2) Par ailleurs, on peut surveiller tous les flux DNS en associant un flux à surveiller, c'est-à-dire créer un compteur CP_T
10 pour chaque terminal et ne jamais l'effacer. On fixe une valeur maximale de CP_T comme $CPTMAX$, $CPTMAX = 2000$.

3) On décide arbitrairement que pour les services autorisés sur le réseau local, comme un service par exemple http, un débit seuil exprimé par un nombre maximum de requêtes DNS, par
15 exemple de 30 par secondes et par terminal est acceptable.

4) On suppose qu'une attaque par canaux cachés par un terminal provoque une brusque élévation du nombre de requêtes DNS de l'ordre de 100 par seconde.

5) On choisit $f(CPT) = \exp(CPT/15)$ comme fonction de
20 retardement (exprimé en milliseconde)

On peut distinguer trois modes de fonctionnement d'un système DNS:

- un fonctionnement normal : l'utilisateur n'est pas mal intentionné et fait un usage du système conforme à ce qui a été
25 prévu.

- un fonctionnement anormal : l'utilisateur est mal intentionné et est probablement en train de commettre une attaque sur le système.

- un fonctionnement sub-normal : l'utilisateur n'est pas mal intentionné mais fait fonctionner ponctuellement le système
30 légèrement au delà des limites prévues.

L'analyse qui suit permet de montrer que le système s'auto-adapte à ces trois cas pour permettre à l'utilisateur d'utiliser correctement le service DNS dans le cas "normal" et

"sub-normal", avec toutefois une légère perte de qualité de service dans le dernier cas; et de bloquer le trafic dans le cas "anormal". L'analyse qui suit n'est pas rigoureuse mais elle permet d'illustrer avec des valeurs numériques une implémentation du procédé, que l'on suivra sur un graphe temporel de la figure 6, représentant l'évolution du nombre de requêtes par seconde en fonction du temps.

A la figure 6, on a représenté l'évolution du nombre de requêtes DNS par seconde en fonction du temps. Du fait de la structure du serveur DNS, le compteur affecté au flux surveillé augmente selon une droite 41. La courbe 42 indique l'arrivée des requêtes pendant l'attaque et la courbe 40 indique le nombre acceptable de requêtes dans le serveur DNS. Enfin la courbe 43 indique l'évolution du nombre des requêtes réémises sur l'interface de sortie de l'équipement de traitement de flux DNS auquel le procédé de protection de l'invention est appliqué.

1) Cas "normal"

Lorsque le système n'est pas sous le feu d'une attaque, il reçoit des requêtes DNS à traiter avec une fréquence de l'ordre de 30 par seconde selon le niveau 40 (figure 6). Le retard appliqué à chaque paquet est alors de $\exp(30/15) = 7,39 \text{ ms}$. Cette valeur montre qu'un paquet sera retardé d'au plus $7,39 \text{ ms}$. Ceci veut dire que pratiquement la totalité des paquets arrivés pendant une durée d'une seconde seront réémis durant la même seconde. En effet, 30 paquets bloqués au plus $7,39 \text{ ms}$ totalisent une durée de $221,7 \text{ ms}$, ce qui est largement inférieur à une seconde. Par conséquent, le compteur *CPT* garde une valeur voisine de 0.

2) Cas "anormal"

Lorsque le système est sous le feu d'une attaque sur un serveur DNS, le procédé de l'invention attribue un compteur *CPT* au flux de l'attaquant, compteur qui va évoluer selon la courbe 41. Par exemple 100 requêtes par seconde, sont émises, en moyenne, sur une seconde. Les paquets seront ralentis de $\exp(100/15) = 785,77 \text{ ms}$. Par conséquent, sur la durée, *CPT* aura

augmenté d'une valeur δCPT , grossièrement comprise entre 50 et 100 puisque très peu des paquets arrivés n'auront été réémis. Ensuite, le retard appliqué aux paquets arrivés la seconde d'après sera de $\exp((100 + \delta CPT)/15) = \exp(\delta CPT) * 785,77 \text{ ms} \gg 20 \text{ s}$.

- 5 On voit donc bien que rapidement le délai appliqué devient complètement bloquant (20 s) et ne cesse de croître jusqu'à atteindre des limites fixées par la valeur maximale de CPT .

3) Cas "subnormal"

- Lorsque le système n'est pas sous le feu d'une attaque, il
10 peut subir simplement une hausse brutale et ponctuelle du nombre de requêtes C'est le cas d'un utilisateur qui visualise une page html qui comporte de nombreuses URL, par exemple 40. Alors CPT va sortir de la zone de « bon fonctionnement » momentanément. Au maximum un retard de $\exp(40/15) = 14,39 \text{ ms}$
15 sera appliqué, ce qui est insensible pour l'utilisateur qui affiche une page html dans un navigateur. De plus, cette valeur ne permet pas à CPT de croître démesurément car les 40 paquets arrivés, même retardés de 14,39 ms, peuvent repartir dans la seconde durant laquelle ils sont arrivés. Un système 'tout ou rien'
20 aurait bloqué complètement le trafic parce qu'il était sortit de la zone de bon fonctionnement ($CPT < 30$). A l'inverse, l'invention n'introduit qu'une légère perte de qualité de service (un retard de 14,39 ms) qui s'estompe au fur et à mesure que le système rejoint le mode de fonctionnement "normal".

- 25 A titre de second exemple, on présente ici comment le procédé de l'invention peut être implémenté dans un serveur Proxy-RADIUS local au réseau à protéger.

- Globalement, le fonctionnement est similaire à la description précédente sur l'implémentation dans le service DNS.
30 En effet, l'idée dans le cas de la limitation des impacts de l'attaque sur l'authentification GSM, est d'utiliser l'invention en coupure du transport de l'authentification GSM. Par conséquent, la description sera plus succincte, et ne s'attardera que sur les points particuliers à l'authentification GSM.

La position la plus simple du mécanisme de contrôle est le proxy-RADIUS pour plusieurs raisons:

L'authentification transite à travers le proxy-RADIUS, quel que soit l'opérateur GSM visé (roaming);

5 Les modifications sur le réseau GSM de l'opérateur sont très lourdes et peuvent avoir un impact fort sur les clients GSM.

Les champs utilisés pour le mécanisme de contrôle seront contenus dans les données du mécanisme d'authentification EAP-SIM. En effet, il est possible de savoir vers quel opérateur
10 l'authentification EAP-SIM est demandée (sous la forme utilisateur@opérateurGSM). Il est donc possible de mettre en place l'invention au niveau du hot spot, pour protéger tous les opérateurs GSM de ce type d'attaque par déni de service.

Ensuite, le mécanisme de contrôle s'exécute dans le cadre
15 normal de l'invention (voir figure 3), qui permet de limiter le nombre de demandes d'authentification grâce à une analyse comportementale sur le transport de l'authentification.

On remarque que la présente invention comporte aussi un usage de détection des usages illicites. En effet, le protocole
20 dans un mode de réalisation de l'invention comporte aussi une étape pour détecter une évolution du débit associé à un flux surveillé caractéristique d'un usage illicite. C'est particulièrement le cas quand le compteur associé à un flux surveillé passe par une valeur maximale, puis se réduit rapidement vers un débit nul.
25 Dans un tel cas, le procédé de l'invention permet de produire une alarme d'un tel usage illicite. Un tel signal d'alarme est transmis à un administrateur de réseau qui peut prendre toute mesure, notamment en tenant un historique des incidents, en cherchant l'identité des auteurs de tels usages illicites et en appliquant
30 toute mesure ultérieure pour réduire l'accès à de tels auteurs.

ABREVIATIONS

DNS: Domain Name Service

EAP: Extensible Authentication Protocol

EAP-SIM: EAP-Subscriber Identity Module

GSM: Global System for Mobile Communications

ICMP: Internet Control Message Protocol

IP: Internet Protocol

5 NAI: Network Access Identifier (identificateur d'accès réseau)

RADIUS: Remote Access Dial In User Service (service des utilisateurs pour la numérotation distante)

TCP: Transport Control Protocol (protocole de commande de transport)

10 UDP: User Datagram Protocol (protocole d'utilisation de datagrammes)

IDS : Intrusion Detection System (système de détection d'intrusion)

15 IPS = Intrusion Prevention System (système de prévention d'intrusion)

RFC : Request For Communication

HTTP : Hyper Text Transfer Protocol (protocole de transfert de fichiers hypertexte)

FTP : File Transfer Protocol (protocole de transfert de fichiers)

20 HTML = Hyper Text Mark-up Language (langage de marquage hypertexte)

REVENDICATIONS

1. Procédé de détection et de prévention des usages illicites de certains protocoles de réseaux sans altération de leurs usages licites, caractérisé en ce qu'il consiste, pour un flux de
5 paquets de données d'entrée, à appliquer une fonction de retardement $f()$ pour chaque paquet, appliquant un retard insuffisant pour gêner un usage licite, mais suffisant pour gêner un usage illicite.

2. Procédé selon la revendication 1, notamment dans un
10 protocole de signalisation, caractérisé en ce qu'il consiste à sélectionner une fonction de retardement croissante avec le débit du flux surveillé, de sorte que si l'usage illicite du protocole à titre de transport de données privées vient à dépasser un débit standard, le retard croît indéfiniment ce qui coupe pratiquement le
15 canal en usage illicite sans gêner les autres flux.

3. Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il consiste, à la détection (21) d'arrivée d'un paquet de données, à déterminer (22) s'il appartient à un flux surveillé et dans la négative, à lui affecter un compteur (CPT).

20 4. Procédé selon la revendication 3, caractérisé en ce qu'il consiste, après la détection (21) d'arrivée d'un paquet de données, à incrémenter (25) le compteur associé au flux surveillé (CPT_N) d'un pas prédéterminé et à appliquer la valeur en cours du compteur comme argument de la fonction de retardement avant
25 de relâcher le paquet de données sur un flux de sortie.

5. Procédé selon la revendication 4, caractérisé en ce qu'il consiste à sélectionner une fonction de retardement à dérivée seconde positive.

6. Procédé selon la revendication 5, caractérisé en ce que
30 la fonction de retardement est une exponentielle dépendant du compteur associé au flux surveillé selon une relation de la forme :
 $f(CPT_N) = \exp(\alpha * CPT_N + \beta)$ avec $\alpha \geq 0$.

7. Procédé selon l'une quelconque des revendications 3 à 6, caractérisé en ce qu'il consiste à déterminer pour le flux

surveillé une valeur maximale admissible de débit $CPTMAX_N$, puis à déterminer si le nombre de paquets en attente d'émission dépasse la valeur $CPTMAX_N$, et en réponse à détruire les paquets en attente.

5 8. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il consiste, pour un système DNS, à s'auto-adapter dans :

- un fonctionnement normal : l'utilisateur n'est pas mal intentionné et fait un usage du système conforme à ce qui a été
10 prévu, le compteur CPT associé gardant une valeur voisine de 0 ;

- un fonctionnement anormal : l'utilisateur est mal intentionné et est probablement en train de commettre une attaque sur le système, le retard appliqué aux paquets DNS augmentant et le compteur CPT associé augmentant ;

15 - un fonctionnement sub-normal : l'utilisateur n'est pas mal intentionné mais fait fonctionner ponctuellement le système légèrement au delà des limites prévues, le compteur CPT restant à des niveaux modérés.

20 9. Procédé selon l'une quelconque des revendications 1 à 7, caractérisé en ce qu'il est implémenté dans un serveur Proxy-RADIUS, local au réseau GSM à protéger, en ce qu'il consiste à déterminer des champs utilisés pour le mécanisme de contrôle contenus dans les données du mécanisme d'authentification EAP-SIM, puis à exécuter le mécanisme de contrôle pour limiter le
25 nombre de demandes d'authentification grâce à une analyse comportementale sur le transport de l'authentification.

30 10. Protocole selon l'une quelconque des revendications 3 à 9, caractérisé en ce qu'il comporte aussi une étape pour détecter une évolution du débit associé à un flux surveillé caractéristique d'un usage illicite et pour produire une alarme d'un tel usage illicite.

surveillé une valeur maximale admissible de débit $CPTMAX_N$, puis à déterminer si le nombre de paquets en attente d'émission dépasse la valeur $CPTMAX_N$, et en réponse à détruire les paquets en attente.

5 8. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il consiste, pour un système DNS, à s'auto-adapter dans :

- un fonctionnement normal : l'utilisateur n'est pas mal intentionné et fait un usage du système conforme à ce qui a été
10 prévu, le compteur CPT associé gardant une valeur voisine de 0 ;

- un fonctionnement anormal : l'utilisateur est mal intentionné et est probablement en train de commettre une attaque sur le système, le retard appliqué aux paquets DNS augmentant et le compteur CPT associé augmentant ;

15 - un fonctionnement sub-normal : l'utilisateur n'est pas mal intentionné mais fait fonctionner ponctuellement le système légèrement au delà des limites prévues, le compteur CPT restant à des niveaux modérés.

9. Procédé selon l'une quelconque des revendications 1 à
20 7, caractérisé en ce qu'il est implémenté dans un serveur Proxy-RADIUS, local au réseau GSM à protéger, en ce qu'il consiste à déterminer des champs utilisés pour le mécanisme de contrôle contenus dans les données du mécanisme d'authentification EAP-SIM, puis à exécuter le mécanisme de contrôle pour limiter le
25 nombre de demandes d'authentification grâce à une analyse comportementale sur le transport de l'authentification.

10. Procédé selon l'une quelconque des revendications 3 à 9, caractérisé en ce qu'il comporte aussi une étape pour détecter une évolution du débit associé à un flux surveillé caractéristique
30 d'un usage illicite et pour produire une alarme d'un tel usage illicite.

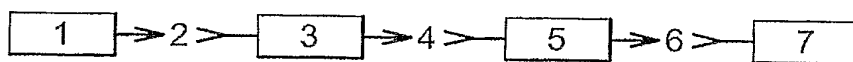


Fig. 1

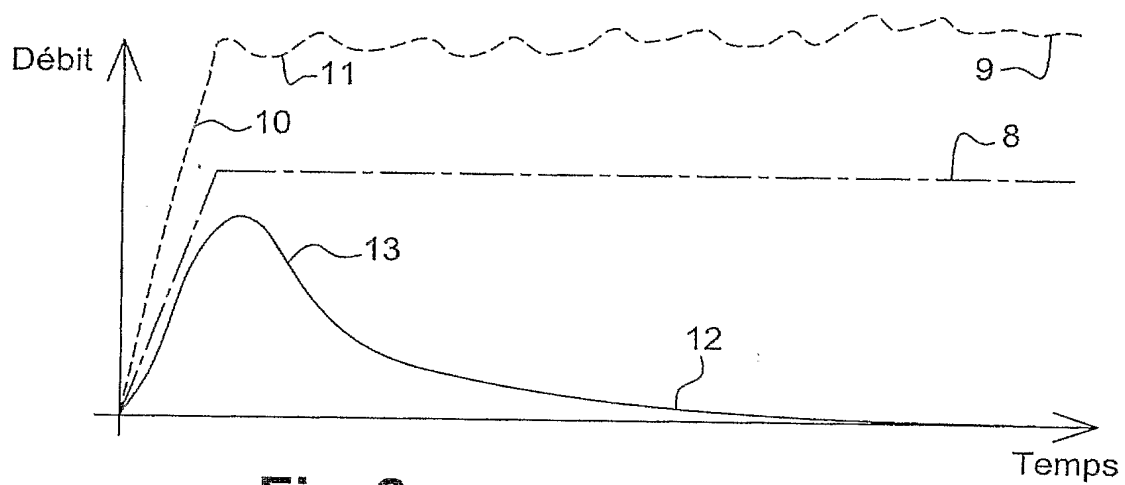


Fig. 2

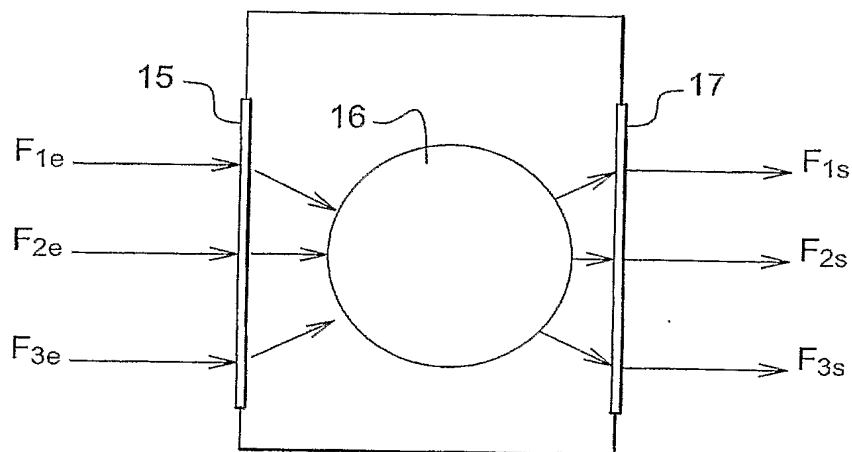


Fig. 3

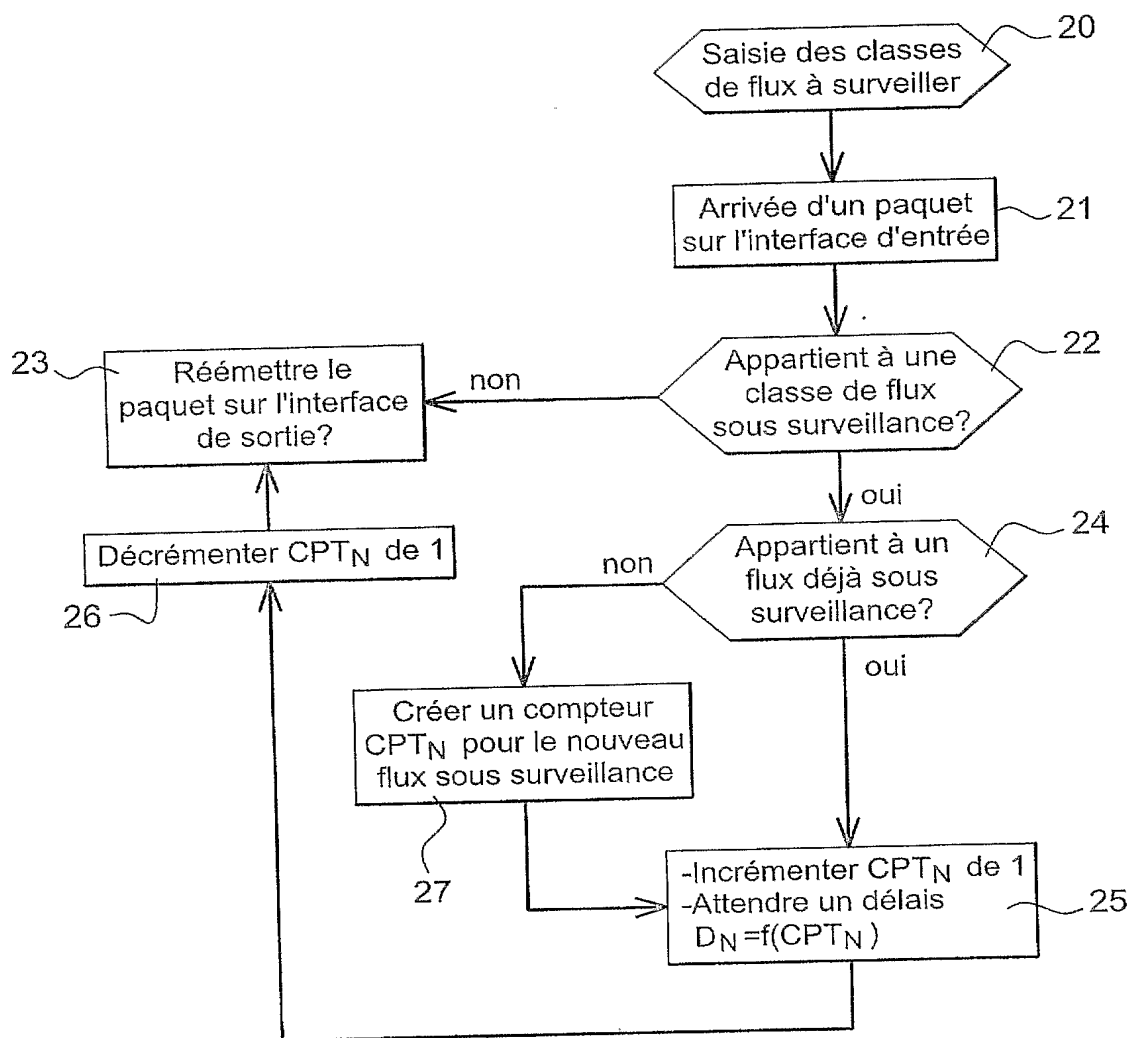
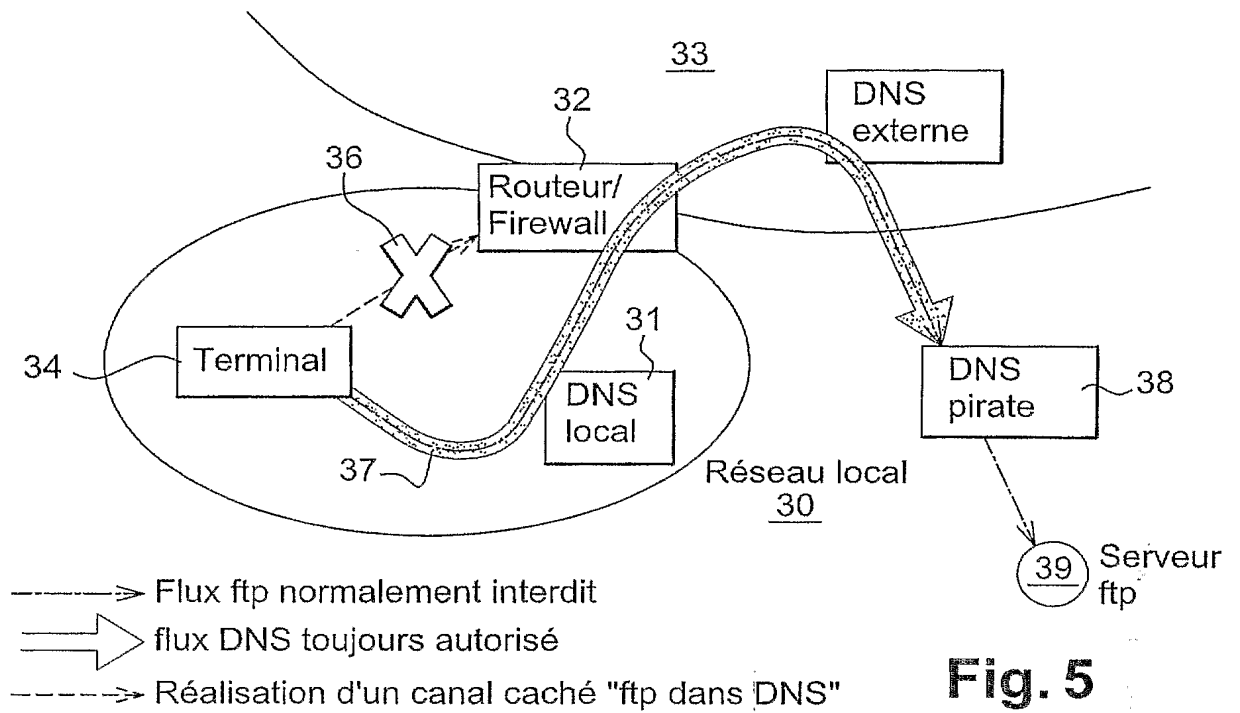
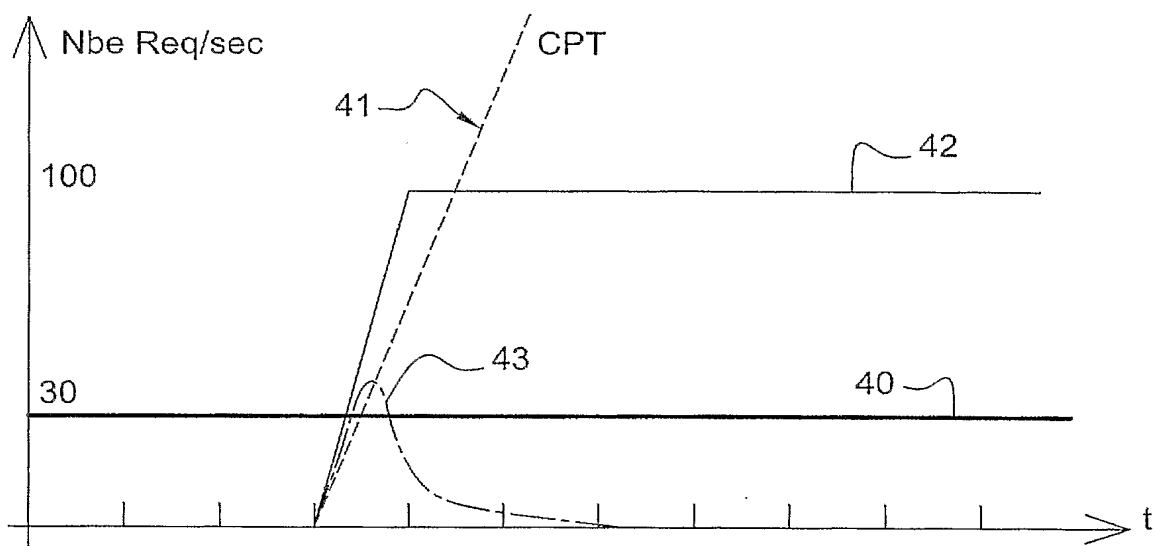
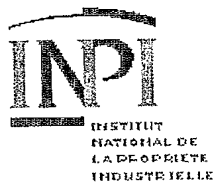


Fig. 4

3 / 3

**Fig. 5****Fig. 6**



BREVET D'INVENTION CERTIFICAT D'UTILITÉ

Désignation de l'inventeur

Vos références pour ce dossier	B-1302-FR
N°D'ENREGISTREMENT NATIONAL	
TITRE DE L'INVENTION	
	PROCEDE DE DETECTION ET DE PREVENTION DES USAGES ILLICITES DE CERTAINS PROTOCOLES DE RESEAUX SANS ALTERATION DE LEURS USAGES LICITES
LE(S) DEMANDEUR(S) OU LE(S) MANDATAIRE(S):	
DESIGNE(NT) EN TANT QU'INVENTEUR(S):	
Inventeur 1	
Nom	CHARLES
Prénoms	Olivier
Rue	104, rue Raymond Losserand
Code postal et ville	75014 PARIS
Société d'appartenance	
Inventeur 2	
Nom	BUTTI
Prénoms	Laurent
Rue	26, rue Saussière
Code postal et ville	92100 BOULOGNE BILLANCOURT
Société d'appartenance	
Inventeur 3	
Nom	VEYSSET
Prénoms	Franck
Rue	184bis, avenue de Verdun
Code postal et ville	92130 ISSY LES MOULINEAUX
Société d'appartenance	

La loi n°78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.